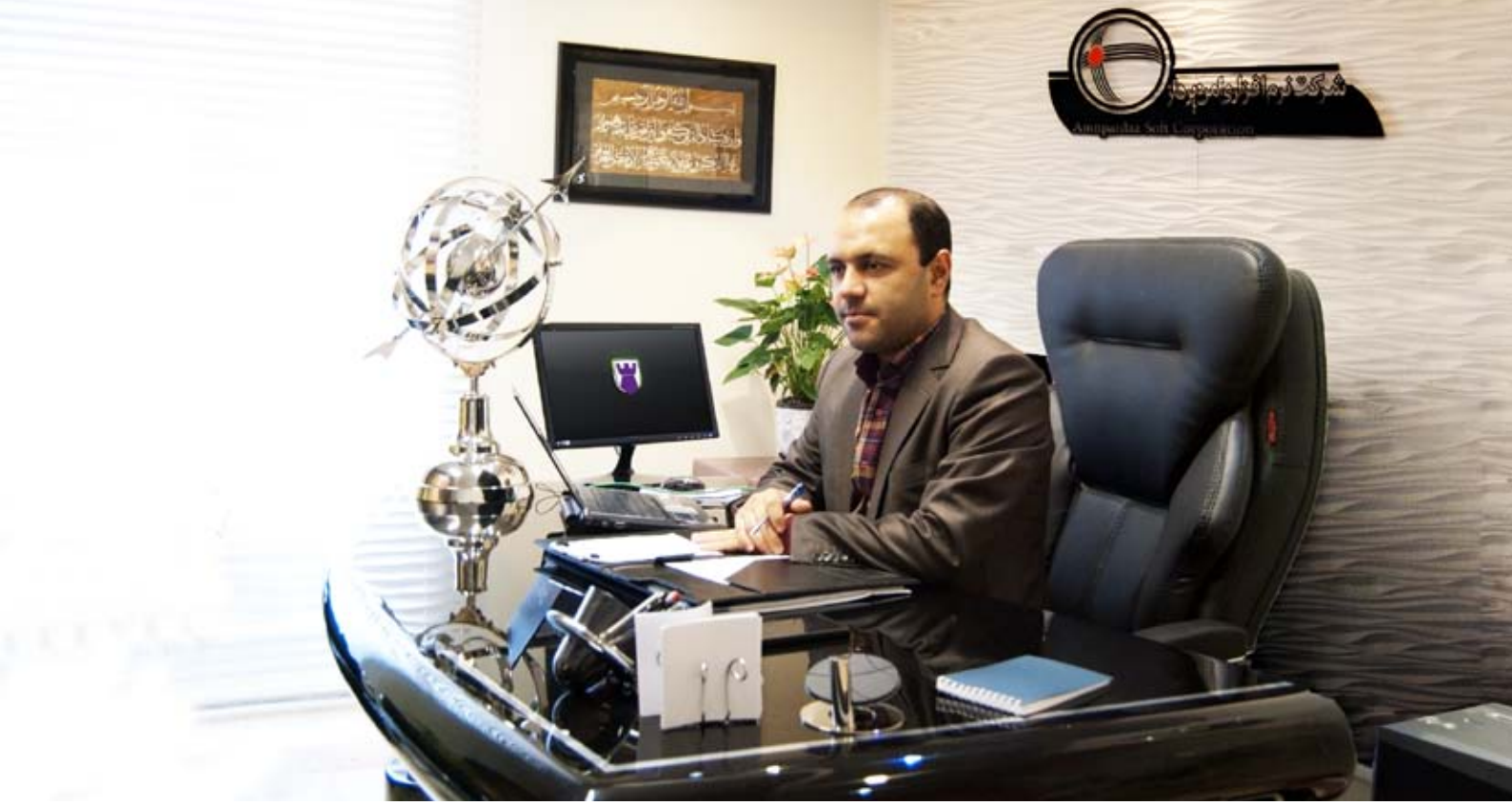
امنیت اطلاعات

بولتن تحلیلی ■ شماره سوم ■ شهریور ۱۳۹۲

شرکت نرم افزاری
امن پرداز



گفت و گو با مهندس عباس حسینی، مدیر عامل شرکت نرم‌افزاری امن پرداز

تجربه‌ی امنیت پایدار

چندی پیش تصمیم گرفتیم با جناب آقای مهندس عباس حسینی، مدیر عامل شرکت نرم افزاری امن پرداز مصاحبه ای داشته باشیم. ایشان علی‌رغم مشغله ی فراوانشان، ما را پذیرفتند و پاسخ‌گوی پرسش هایمان بودند. پرسش هایی که نه تنها راه و منش شرکت امن‌پرداز را برای شما خوانندگان محترم بیان خواهد نمود، بلکه به ما نیز شور و شعف بیشتری برای ادامه‌ی این پروژه را داد و انرژی زائدالوصفی که ما را به تفکر در مورد رسالت های شرکت وادار کرد.

• شرکت امن پرداز چه زمانی و چگونه تاسیس شد و شروع به کار کرد؟

ما از سال ۱۳۸۴ فعالیت کاری خودمان را در امن پرداز شروع کردیم و ثبت شرکت در سال ۱۳۸۳ انجام شد. هسته ی اصلی تشکیل دهنده ی امن‌پرداز افرادی بودند که پیش‌تر مسئولیت شبکه را در دانشگاه شهیدبهشتی برعهده داشتند، یعنی درواقع تخصص این افراد در زمینه ی پشتیبانی شبکه و شبکه های کامپیوتری بود. لذا اولین فعالیتی که جهت ارتزاق شرکت و همچنین تامین مایحتاج و هزینه های آن انجام شد، قراردادهای پشتیبانی بود و در نهایت هدف این بود که درآمد های حاصله از قراردادهای شبکه ای صرف تولید محصولات نرم افزاری شود. همانطور که می دانید نرم افزار یک نیاز روز افزون جامعه ی بشری است؛ در قرن ۲۱ هیچ صنعتی را نمی توان یافت که تولیدکنندگان پیشرو آن از نرم افزار بی بهره یا بی نیاز باشند، به‌عبارتی نرم افزار یک نیاز روزافزون و اجتناب ناپذیراست. بحث امنیت در نرم افزار یک امر حیاتی و لازم الاجرا است. همانطور که می دانید افرادی که دربخش امنیت هر حوزه ای کار می‌کنند، اصولا خبره‌ی آن فن می باشند، زیرا که در امنیت باید ابتدا تمام ریزه‌کاری های یک مسئله را دانست و با آن آشنا بود تا بتوان در مورد امنیت و امن سازی آن زمینه فعالیت کرد. اصولا سوءاستفاده از یک مطلب بسیار آسان تر از بهینه سازی آن است، پس اگر شرکتی ادعا کند که قفلی را امن می‌کند، باید در مقابل تمام حملات و ضربه ها مصونیت کافی را ایجاد نماید.

بنابراین "شرکت نرم افزاری امن پرداز"، شرکتی است نرم افزاری که امنیت در حوزه‌ی نرم افزار را به عنوان هدف و ماموریت خود در حوزه‌ی فضای مجازی انتخاب کرده است.

• میزان پیشرفت شرکت را از زمان تاسیس، چه مقدار می بینید؟ لطفا مقایسه ای کلی از زمان تاسیس تا امروز از حیث تعداد نفرات، پروژه ها و سرمایه ارائه می دهید ؟

میزان پیشرفت شرکت از زمان تاسیس بسیار خوب بوده و این مقدار حتی بیشتر از پیش بینی و تصورات ما بوده است. دلیل این پیشرفت نیروهای قابلی بودند که برای همکاری با ما در شرکت فعالیت داشتند. همچنین من در شروع این کار تنها بودم و شرکت را تنها و به اتفاق دو نفر از اعضای خانواده‌ام ثبت کردم و هدف این بود که شرکا در طول کار انتخاب شوند، که همین اتفاق هم افتاد. در زمان تاسیس شرکت تعداد همکاران ۵ تا ۶ نفر بود که امروز امن پرداز قریب به ۱۰۰ همکار خبره دارد. این میزان رشد در حدود ۸ سال، یعنی از سال ۱۳۸۴ تا سال ۱۳۹۲ رخ داده است.

• به طور کلی ساختار شرکت به چه نحوی است؟

ساختار و سازمانی که پادویش در آن رشد کرد، یک ساختار کاملا دانش بنیان است و این محصول در محیطی فراگیرنده و خودآموز تولیدشده است. ما حتی سعی می‌کنیم تمام فعالیت های داخلی این سازمان را مبتنی بر IT و خودکار کنیم. به طور مثال چندی پیش همکاران، سامانه ای نرم افزاری برای ثبت سفارش ناهار و پرداخت تهیه کرده‌اند. یعنی تیم امن پرداز در این حد اهتمام دارد که کلیه ی فعالیت ها، خودکار بوده و به معنای واقعی کلمه IT Base باشد.

• لطفا از چارت و کادر سازمان و بخش‌های مختلف آن اگر مایلید، توضیحی بدهید.

به صورت کلی تیم ما از ساختاری مناسب برای توسعه‌ی نرم افزار تشکیل شده است که در این تیم افرادی با مسئولیت های طراحی، تحلیل و معماری مشغول هستند. افراد دیگری وظیفه ی مستند سازی ساخت یک محصول نرم‌افزاری را بر عهده دارند. تیم های دیگری

مسئول تست و کنترل کیفیت محصول می‌باشند. تیم پشتیبانی نیز از جمله تیم‌های مهم در رابطه با سرویس‌هایی که به مشتریان ارایه می‌شود، است. همچنین با توجه به نوع محصولی که در حال تولید می‌باشد، تیم فنی به نفرات متخصص، تیم‌ها و گروه‌های کاری مرتبط و متخصص هر فعالیت تفکیک می‌شوند. مدیریت کل، امور مالی، امور بازرگانی و خدمات می‌باشند.
تمام هدف ما این است که حدالمقدور و به صورت مستمر نسبت به بهبود فرآیندهای کاری و ارتباطات فی‌مابین تیم‌ها و واحدها اقدام کنیم و این مهم را عامل اصلی گسترش و توسعه‌ی محصول چه از بعد فنی و چه از بعد تجاری آن میدانیم.

• چه شد جرقه‌ای در ذهنتان ایجاد شد که آنتی ویروس بسازید و از کجا این پروژه آغاز شد؟ علی الخصوص با توجه به حضور شرکت‌های خارجی سازنده‌ی آنتی ویروس، تا چه اندازه این مقدار موفقیت را پیش بینی می‌کردید؟
پروژه‌ی آنتی ویروس از این رو پروژه‌ی انتخابی ما بود که گمان می‌کردیم بازار مناسبی را در داخل کشور دارد. بازار کشور ما یک بازار دولتی است، یعنی اگر دولت متقاضی یک محصول باشد می‌شود گفت آن محصول در بازار حرفی برای گفتن دارد. نیازی روزافزون در خصوص بهره‌مندی از یک ضدبدافزار بومی در بدنه‌ی نظام شکل گرفت و به این دلیل این گزینه را به عنوان پروژه پذیرفتیم و در آن سرمایه‌گذاری کردیم. دلایل دیگری که ما را به این سمت سوق داد عبارتند از:
-شرکت‌های خارجی آنتی ویروس در بازار ایران سابقه‌ی خیلی خوبی ندارند و متاسفانه سابقه‌ی خیانت به مشتری در کارنامه‌شان ثبت شده است. امروزه هر شهروند ایرانی می‌داند که بنا به دلایل سیاسی آنتی ویروس های خارجی خود را در سوءاستفاده از اطلاعات محق می‌دانند و محدودیتی در این زمینه برای خودشان قائل نیستند.
-همچنین تجربه نشان داده که این شرکت‌ها بسیاری از بدافزارهایی که به عنوان یک جنگ‌افزار مجازی مشهور شده‌اند را با مقاصد سیاسی ترکیب کرده‌اند و عمدا آن‌ها را شناسایی نکرده که به کاربران ایرانی ضربه وارد کنند.
اما در هر صورت انتخاب ما در خصوص تولید آنتی ویروس ملی، یک انتخاب تجاری است، یعنی تصور می‌کنیم که سود مناسبی را به همراه دارد. البته تولید برای هر کشوری فوایدکوتاه مدت یا میان مدت و دراز مدت مختلفی دارد. مسائلی که تاکنون ذکر شد از دسته مسائل کوتاه مدت یا میان مدت بود. تسلط بر فن‌آوری آنتی ویروس، تسلط بر یکی از فن‌آوری‌های پایه در حوزه‌ی امنیت اطلاعات است که به عنوان یک بستر می‌توان از آن استفاده نمود. موفقیتی که امروز و در این مرحله در بحث پروژه‌ی ضد ویروس کسب کرده‌ایم، معطوف به گذر از چالش‌ها و مشکلات فن‌آورانه بوده است و این بدان معنا است که ما به فن‌آوری های لازم برای تولید فنی محصول رسیده‌ایم. قسمت عمده‌ای از بازارپسندی یک محصول به بازخوردها و نظراتی که مشتریان منتقل می‌کنند بازمی‌گردد که درنهایت باعث پسند مشتری می‌شود. اما موفقیت بازرگانی محصول هنوز به دست نیامده و این خود مستلزم داشتن سیاست‌های بازرگانی و تبلیغاتی درست است. ورود مناسب محصول به بازار، کسب اعتماد مشتریان و موارد متعدد دیگر، در بازار سازی نقش مناسبی می‌تواند داشته باشد.

• اصلا چرا پادویش بخریم؟
اگر منظور کابران خانگی است، ما می‌گوییم نیازی به خرید پادویش نیست زیرا ما آن را به صورت رایگان در اختیارتان قرار داده‌ایم. رایگان بودن پادویش برای کابران خانگی دلایل مختلفی دارد. اول اینکه ما در بازاری زندگی می‌کنیم که برای اصلی‌ترین محصولات مثل سیستم عامل، محصولات کاری مثل آفیس و نرم افزارهای عمومی پولی پرداخت نمی‌کنیم. حال پرداخت پول برای نرم‌افزاری که روی یک پلات‌فرم رایگان می‌نشیند کمی غیرمنطقی است. دوما به دلیل عدم رعایت کپی رایت، محصولات رقبای خارجی در ایران رایگان یافت می‌شود و اینکه ما خود محصولمان را رایگان ارائه کنیم، عاقلانه‌تر به نظر می‌رسد.
سوم نفعی که این طرح برای شرکت دارد این است که وقتی محصول مدنظر به دست کاربران خانگی می‌رسد با نظرات و بازخوردهایی که به ما اعلام خواهد شد کمکی به بهبود خواهدکرد. یعنی این خود یک تست عمومی همگانی برای محصول خودمان خواهد شد، راهی که دقیقا تمام تولیدکنندگان محصولات بزرگ در دنیا رفته‌اند.
و اما نکته‌ی چهارم که از سایر نکات مهم‌تر هم هست، اینکه آنتی‌ویروس‌ها با استفاده از یک فن‌آوری به اسم پردازش ابری اقدام به مراقبت از بدافزارها و تهدیدات جدید می‌کنند. این موضوع هم بدون اینکه آنتی ویروس توزیع عمومی شده باشد عملا امکان‌پذیر نیست، به عبارتی ما تا در بدنه‌ی فضای مجازی یک کشور حضور نداشته‌باشیم، نمی‌توانیم از وضعیت ویروس‌ها و تهدیدات و مشکلات ناشی از آن‌ها مطلع شویم. بنابراین حسن دیگر این طرح برای شرکت این است که می‌تواند منبع بسیار مناسبی برای کشف مخاطرات و تهدیدات روز جامعه‌ی IT کشور باشد.

• آیا پادویش در رقابت با بقیه آنتی‌ویروس‌ها است؟ به چه نحوی و با چه چشم‌اندازی به رقابت با سایر شرکت‌ها خواهد پرداخت؟
ما پادویش را با دید کاملا رقابتی طراحی کرده‌ایم. یعنی ما در طراحی و معماری‌مان، محصولی با قابلیت رقابت کامل و پتانسیل‌های فنی بالاتر از محصولات مشابه برنامه‌ریزی کردیم و در این سمت نیز در حال حرکت هستیم.
تجربه نشان می‌دهد که یک شرکت آنتی ویروس برای حصول موفقیت نیاز به سابقه‌ای با بازه‌ی ۱۰الی۱۵ ساله دارد و حداقل باید به مدت ۵ سال در بازار حضور داشته باشد. با توجه به این مطلب که ما هنوز به صورت رسمی وارد بازار نشده‌ایم، بنابراین با یاری خداوند برنامه‌ای بین ۵ الی۱۰ ساله برای فراگیرشدن و موفقیت پادویش پیش بینی می‌کنیم.

• از افتخاراتی که شرکت و نخبگانتان کسب کرده‌اند، برایمان بگویید.
به غیر از محصولاتی که امن‌پرداز موفق به تولید آن شده است، شرکت افتخارات نسبتا زیادی در حوزه‌های فنی داشته است. عمده‌ی محصولاتی که ما تولید کرده‌ایم، یا برای بار اول داخل کشور تولید شده بود و یا هم تراز این محصولات، محصول دیگری تابه‌حال در کشور نداشتیم. بنابراین اولین و مهم‌ترین افتخار ما این است که سعی می‌کنیم خود را از نظر فنی در تراز شرکت‌های درجه‌ی یک دنیا تعریف کنیم. البته این امر از نظر تجاری بسیار سخت است و همه‌ی عوامل نیز تنها در دست ما نیست.

• بدترین اتفاقی که به زعم شما می‌تواند برای شرکتتان بیفتد چیست؟
بدترین اتفاقی که ممکن است برای شرکت بیفتد تغییر فرهنگ سازمانی آن است که عامل اصلی خلاقیت تیم‌ها و یک فرهنگ سازنده و تولید محور می‌باشد. مهمترین عامل موفقیت یک موجودیت حقوقی که یک شخصیت منحصر به فردی را نیز تداعی می‌کند، این است که روح سازمانی آن سالم، مثبت، پیش‌رونده و مستعد ارتقا و رشد باشد. خروجی خوب و باکیفیت یک مجموعه، نشان‌دهنده‌ی ورودی خوب و

در نتیجه رفتار با کیفیت یک سازمان است و همیشه بهترین محصولات را بهترین شرکت ها تولید می‌کنند؛ که این "بهترین شرکت ها" قطعا در وهله ی اول، در بعد داخلی و سازمانی از بهترین ها هستند. این مهم ترین مسئله ای است که باید همیشه هم از آن مراقبت کرد. هرچند مسائلی مانند مشکلات مالی، فضای بد کسب و کار و اتفاقات مالی می تواند تهدیدات بزرگی را برای شرکت بوجود آورد، اما این تهدیدات با توان مندی و بنیه ی مالی شرکت درصد ریسک کمتری را به خود اختصاص می دهد و شرایطی پیش می آید که می توان به تیم ها گفت که تا سال دیگر هم اگر پروژه ای نداشته باشیم، مشکل خاصی ایجاد نخواهد شد، تا تیم ها با آسودگی خاطر به ادامه ی پروژه بپردازند. بنابراین بزرگترین مسئله برای یک شرکت این است که سازمان از درون پوسیده و پوک شود که باید نسبت به این موضوع بسیار هوشیار بود و مراقبت کرد.

• و یک سوال کمی اختصاصی، برایتان پیش آمده که به ورشکستگی فکرکنید؟ و چگونه بر این حس غلبه می‌کنید؟

حقیقت این است که نه بنده و نه هیچ شخصی مشابه بنده که قدم در این راه گذاشته، هرگز به شکست فکر نکرده است. اصولا شکست و ورشکستگی قبل از هر چیزی یک امر ذهنی است، یعنی انسان خود می پذیرد که چه زمانی شکست خورده است. بنابراین ما هرگز به ورشکستگی فکر نخواهیم کرد، که متعاقب آن حسی به وجود بیاید که بخواهیم بر آن غلبه کنیم. اما واقع بینی و توجه به شرایط ایجاب می کند که مجموعه را از نزدیک شدن به پرتگاه و یا انجام کارهای پرخطر دور کنیم و پیش بینی مناسبی را برای آینده داشته باشیم که تضمین های حداقلی را برای پرسنل و کلیه ی کسانی که با امن پرداز در ارتباط هستند و حتی مشتریان به ارمغان بیاوریم. نکته ی بسیار مهم این است که شرکت باید بتواند به میزانی از ارزش مندی برای مشتریانش برسد که مشتریان خود نتوانند قطع خدمات شرکت را تاب بیاورند، در این صورت خود آن ها هیچ‌گاه نمی‌گذارند که شرکت به ورشکستی برسد. همان‌گونه که در طول دوره ی کاری ما هم بارها به مشکلات مالی خیلی زیاد برخورده بودیم، اما از بین مشتریان ما افرادی بودند که خدمات و محصولاتمان را پیش خرید کردند و با سرمایه‌گذاری هایی به این نحو، باعث شدند که از آن بحران عبور کنیم و در طول دوران همکاری به عنوان یک همکار استراتژیک و یک شریک بی‌بدیل برای هم تبدیل شدیم.

• به کسانی که میخواهند کسب و کاری پژوهشی را شروع کنند، چه توصیه هایی دارید؟

به این عزیزان پیشنهاد می‌کنیم که هدف خود را در این مسیر بر ارائه ی خدمت صادقانه و ارتقاء سطح کیفی محصولات یا خدماتی که ارائه می دهند، متمرکز کنند و همچنین صرفا جنبه های مالی را برای خود هدف‌گذاری نکنند، زیرا که کار پژوهشی پروسه ای دارد که می بایست در آن علاقه ی خدمت به مردم را در وجود خود داشته باشیم و گرنه در نیمه های راه قطعا به بن بست خواهیم رسید.

• و در آخر اگر بخواهید ایرانی ها را متقاعد به خرید پادویش کنید

...

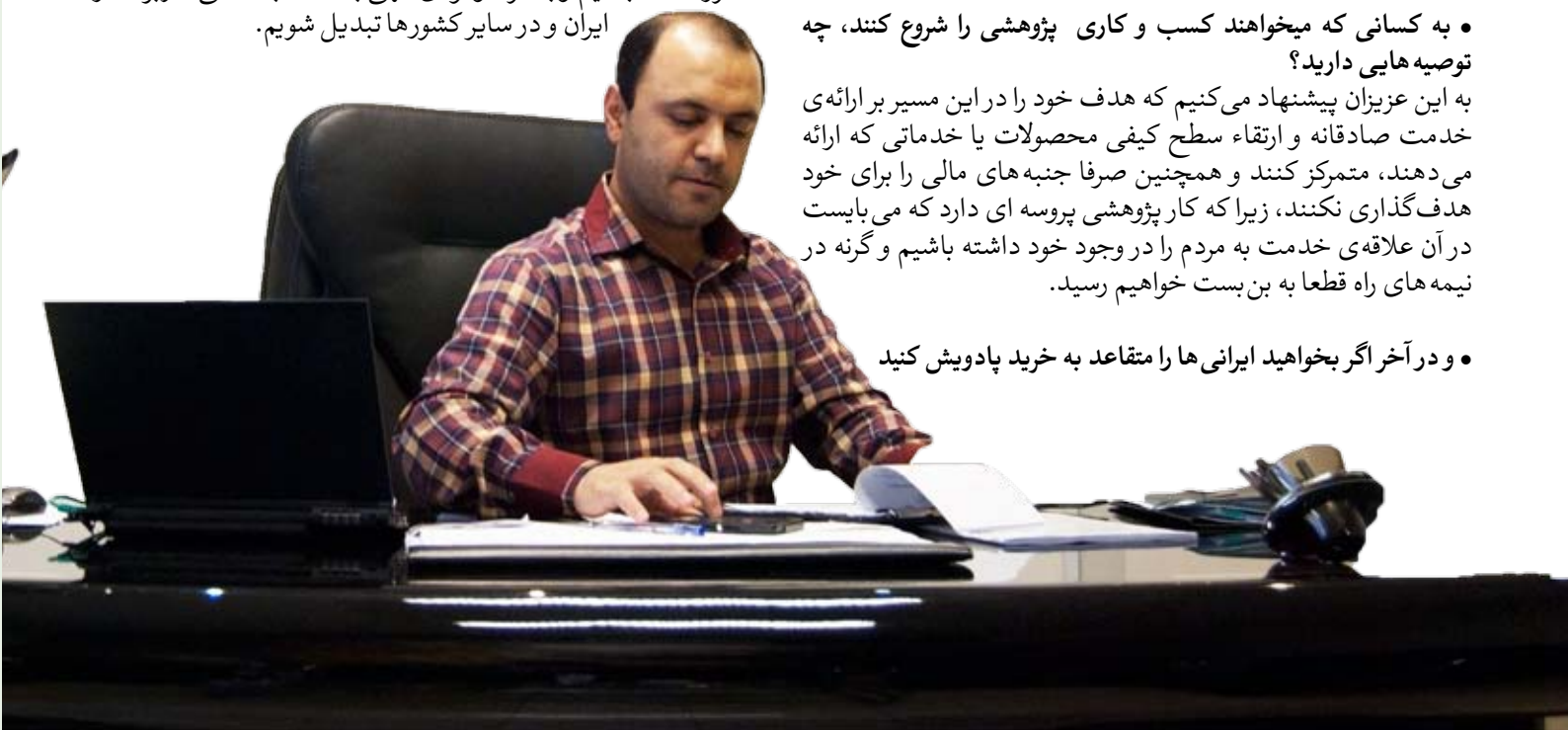
همانطور که گفتیم پادویش فعلا به صورت رایگان در اختیار مشتری های خانگی قرار گرفته است، پس نمی‌گوییم که پادویش را بخرید؛ از آن ها خواهش می‌کنیم که به عنوان یک محصول رایگان از آن استفاده‌کنند و مطمئن باشند که این محصول به لطف خداوند و با همت هم وطنان به زودی محصولی جهانی می شود که باعث افتخار همه ی ایرانی ها خواهد شد. استفاده ی رایگان آن ها از این محصول بهترین کمک برای توسعه ی این نرم افزار ضد بدافزار است.

همچنین از آن ها می‌خواهیم که توجه داشته باشند محصولی را استفاده می‌کنند که هنوز چند ماه از عمرش نگذشته است و در مقایسه با محصولاتی که چندین و چند سال از عمرشان می‌گذرد، به سن و تجربه ی این کودک نوپا و این تیم جوان توجه کنند و به ما فرصت دهند و توجه‌کنند که این محصول، محصولیست که ۱۰۰٪ در داخل کشور طراحی، معماری و ساخته شده است، لذا ما هیچ محدودیتی در ارائه ی مولفه های آن از جهت توسعه و همچنین ویژه سازی هایی برای نیازهای ایرانیان نداریم.

تصور من درمورد مشتریان سازمانی هم این است که تجربیات ناموفق آن ها در استفاده از محصولات خارجی دلیل مکفی می باشد که به سمت استفاده از یک محصول داخلی حرکت کنند و قطعا هنگام تنها ماندن در مواقع بحران، حضور یک شرکت داخلی که از فن‌آوری لازم برای حمایت آن ها برخوردار است، میتواند کمک بزرگی به حساب بیاید.

همچنین به توزیع کنندگان محصولات خارجی عرض می‌کنم که ما صمیمانه از آن ها دعوت می‌کنیم با شرایط مشابه فروش محصولات خارجی، حاضر به همکاری با آن ها هستیم. سیاست کلی ما درعرضه ی محصولات خصوصا آنتی ویروس، عرضه از طریق نمایندگی های فروش هست و نه عرضه ی مستقیم؛ بنابراین نمی‌خواهیم حضور یک آنتی ویروس بومی را محملی برای مونوپل شدن و انحصار محصول در بازار تلقی کنند.

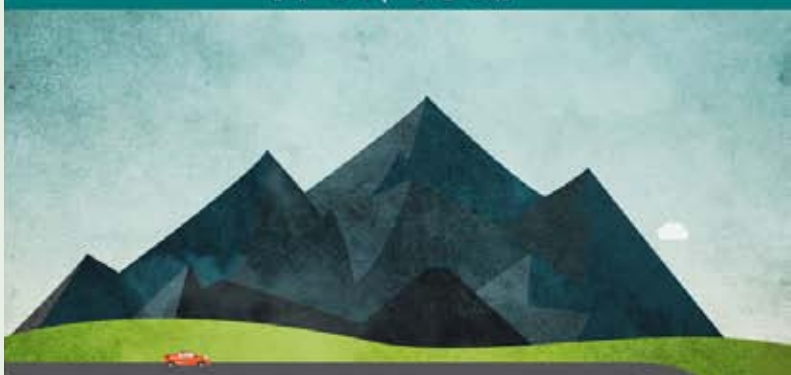
اعتقاد قلبی‌ام این است که ایرانی ها وقتی به این باور و درک برسند که این محصول قابل رقابت، و دارای کیفیت مورد انتظار آن ها است، قطعا با تعصب و غیرت ایرانی از این محصول حمایت می‌کنند و تصور من بر این است که غالب مشتری های ما به این سمت حرکت خواهند کرد. ما وظیفه ی خودمان می‌دانیم که در یک رقابت سالم در بازار، همواره حضور داشته باشیم و با حول و قوه ی الهی به انتخاب اصلی کاربران در ایران و در سایر کشورها تبدیل شویم.



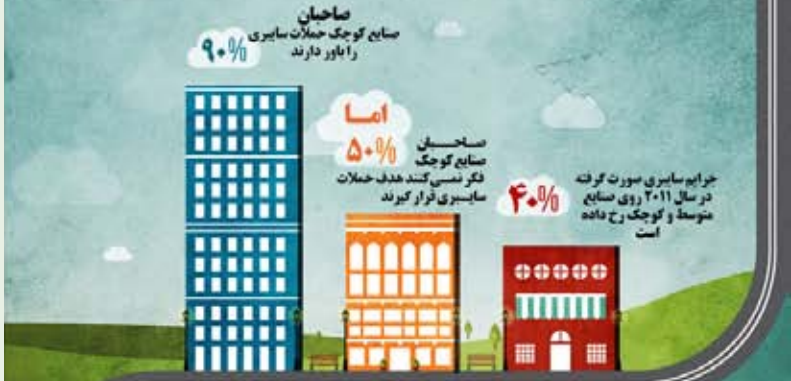
....جرایم سایبری

حفاظت از صنایع کوچک در برابر تهدیدات سایبری ••••••••

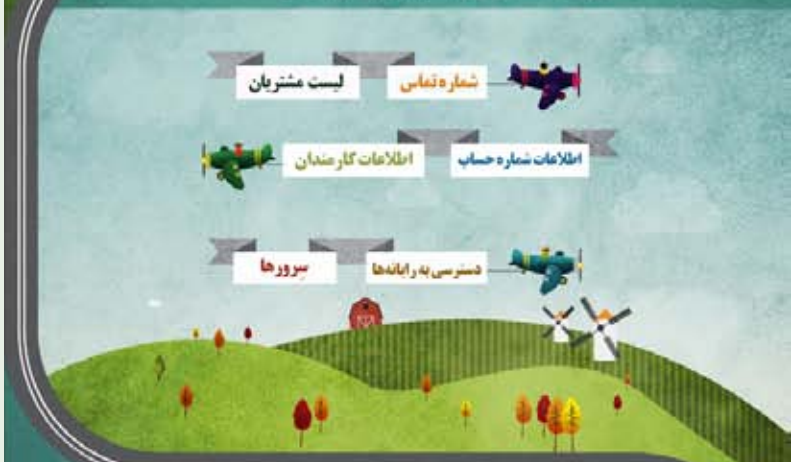
هکرها حتی به صاحبان صنایع کوچک هم رحم نمی‌کنند.
امروزه باید این تهدیدات را شناخت و برای پیشگیری از حملات سایبری که منجر به جرایم سایبری می‌شوند چاره‌ای اندیشید.



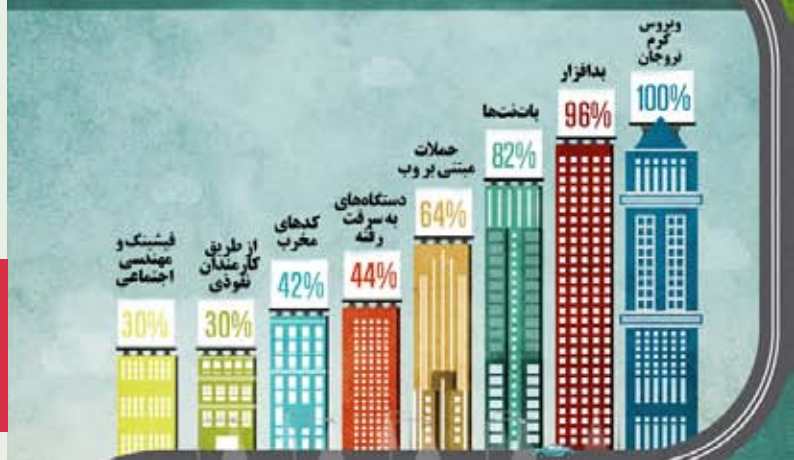
تهدیدات سایبری فقط مختص صنایع بزرگ نیست.



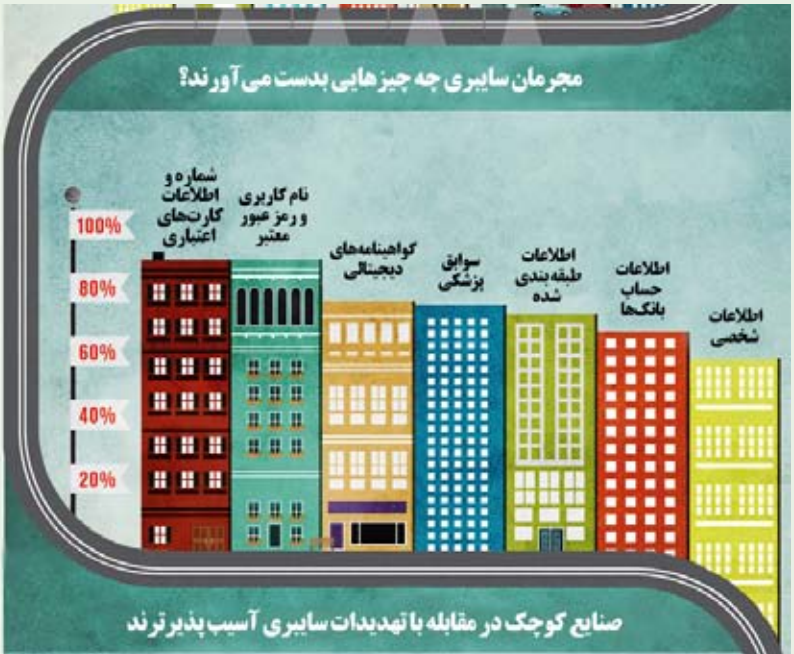
مجرمان سایبری به دنبال چه چیزی هستند؟



صنایع با چه حملاتی روبه‌رو می‌شوند؟

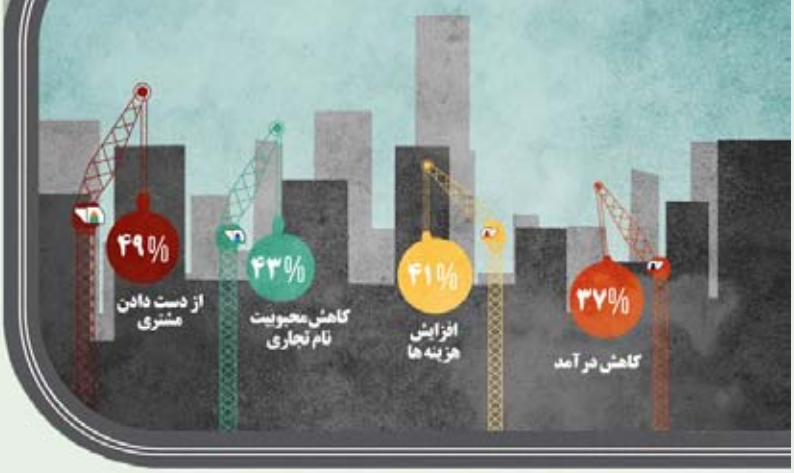


مجرمان سایبری چه چیزهایی بدست می‌آورند؟

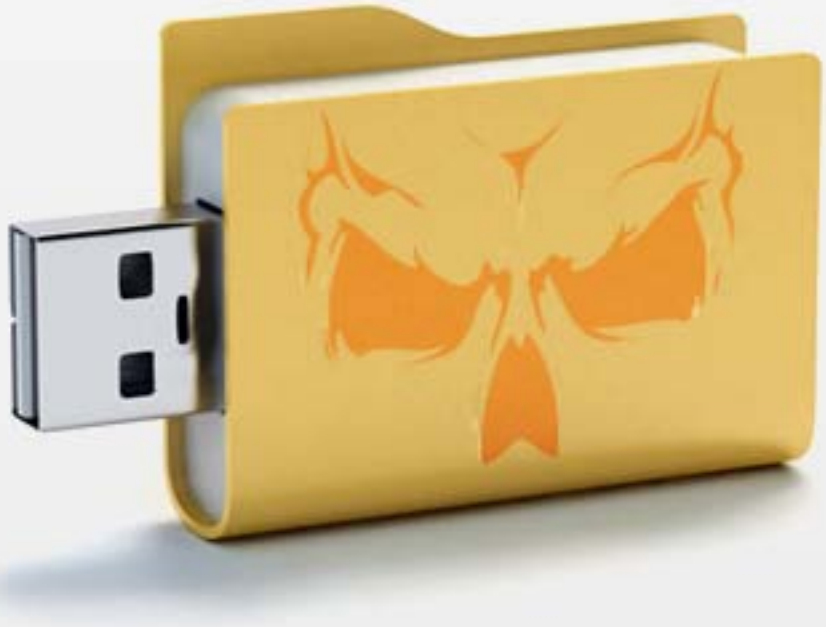


صنایع کوچک در مقابله با تهدیدات سایبری آسیب‌پذیرترند

پیامدهای از دست دادن اطلاعات چیست؟



گرداب



تحلیلی بر بد افزار گامارو

این پوشه های خطرناک...

مقدمه ای بر کرم Gamarue

این بدافزار نوعی کرم است که از طریق درایو قابل حمل، خود را منتشر می‌کند و با دانلود نسخه‌ی جدیدی از خود به روز می‌شود. در درایو قابل حمل، پوشه‌ای بدون نام و با آیکونی مانند آیکون همین درایو توسط این کرم ساخته شده و تمامی محتویات درایو قابل حمل، به این فولدر انتقال داده می‌شود؛ سپس یک فایل میانبر با نام و با آیکون این درایو ایجاد می‌شود. در روبروی نام، اندازه‌ی این درایو در پرانتز به نمایش در می‌آید که کاربر برای دسترسی به فایل‌ها ناچار به اجرای این میانبر شود و بااجرا، علاوه بر نمایش دادن فایل‌هایی که در پوشه بدون نام قرار دارند، کرم نیز برروی سیستم اجرا گردد. این بدافزار دارای فایل DLL با پسوند init*، fat.* یا fat32.*، nil.* و... بوده و فایل‌های دیگری نیز با نام‌های desktop.ini و Thumbs.db با ویژگی‌های مخفی، سیستمی و فقط خواندنی در مسیر درایو قابل حمل ایجاد می‌نماید.

مراحل اجرای کرم Gamarue

- اجرای لینک (lnk.*) توسط کاربر جهت مشاهده‌ی محتویات درایو قابل حمل
- بارگذاری فایل dll با استفاده از Rundll32
- استفاده از فایل desktop.ini به منظور بارگذاری کد اصلی (این فایل می‌تواند بصورت رمز شده باشد)
- دانلود فایل Thumbs.db بعد از نصب درایو قابل حمل به سیستم و ذخیره‌ی آن در این درایو
- ساخت پوشه ای با نام‌های MSI، TMp، Temp در درایو اصلی (Root) و استخراج فایل اجرایی trustedinstaller.exe از درون فایل فشرده شده‌ی thumbs.db
- اجرای فایل Trustedinstaller.exe
- ایجاد فایلی جدید بانام msiexec.exe در مسیر temp کاربر و درون پوشه‌ای که نام آن تصادفی می‌باشد
- کپی‌کردن فایل TrustedInstaller.exe با نام تصادفی و با پسوند tmp. در مسیر temp کاربر([Random_name.tmp])
- خواندن مکرر از فایل <Random_name.tmp> و ذخیره بر روی بافر خود و کدکردن محتویات
- ساخت مقداری بانام "Imagebase" برای محتویات کدشده فایل TrustedInstaller و در کلید HKCU\Software
- پاک‌کردن فایل <Random_name.tmp>
- اجرای فایل msiexec.exe

فرآیند msiexec

عملکرد یکی از فرآیندهای معروف این است که wuauclt.exe (در سیستم عامل ۳۲ بیتی) یا Svchost.exe (در سیستم-عامل ۶۴ بیتی) را به صورت یک فرآیند suspend ایجادکرده و سپس کد رمزگشایی شده خود را به فرآیند ایجادشده تزریق می‌کند. (این تکنیک اولین بار در بدافزار Duqu استفاده شد)

فرآیند Wuauclt.exe یا Svchost.exe

کپی کردن فایل msiexec.exe با نامی تصادفی در مسیر temp سیستم به شرح زیر:

• ساخت مقداری با نام عددی، به صورت تصادفی و با مقدار مسیر فایل فوق، در کلیدی با آدرس HKLM\software\microsoft\windows\currentversion\Policies\Explorer\Run جهت بقای بد افزار

• اگر نسخه های جدیدی از فایل های خود موجود باشد، برای دانلودکردن آن ها به سرورهای زیر متصل خواهد شد و مقادیری با نام های DOS_STUB، Imagebase و IMAGE_FILE_HEADER در کلید رجیستری HKLM\Software\Microsoft برای فایل های دانلودشده می سازد. ولی اگر نتواند به این سایت ها متصل شود و نسخه های جدید خود را دانلود کند، برای محتویات فایل های خود این سه کلید را تولید خواهد کرد:

http://a.s***.in/mzbnx*****
http://b.s***.in/smob*****
http://c.s***.in/suhqk*****

و با اتصال به سایت های زیر قصد دانلود فایل اجرایی را خواهد داشت که پس از دانلود فایل آنها را اجرا خواهدکرد.

http://hzm****.biz/ldr.php
http://hzm****.in/ldr.php
http://hzm****.ru/ldr.php
http://hzm****.com/ldr.php
http://hzm****.nl/ldr.php

علاوه بر این موارد باید اشاره کرد که در نسخه های جدید، این کرم همزمان پردازه پدری را به پردازه های svchost.exe ، wuauclt.exe و به پردازه دیگری تزریق می‌کند و عملیات یکسانی همچون پردازه های svchost.exe ، wuauclt.exe را انجام می دهد. دلیل مهمی که دو پردازه بصورت همزمان از پردازه پدر ایجاد می شوند، بقای آنهاست. بنابراین اگر یکی از این دو پردازه به هر دلیلی توسط سیستم یا کاربر پایان یابد، دیگری دوباره آن را بوجود خواهد آورد.

روش های جلوگیری از تحلیل

در برخی نسخه ها از این روال به شرح زیر استفاده می‌کنند:

• پردازه های در حال اجرا، سیستم را رمز نموده و آن را با نام های رمز شده‌ی نرم افزارهای مانیتورینگ و شبیه سازهای مجازی (VirtualBox، VMware و...) مقایسه می‌کنند.

• به دست آوردن نام هارد دیسک از رجیستری و مقایسه آن با سه رشته qemu، vbox، vmwa، که وجود شبیه سازهای مجازی را تشخیص می دهد.

• استفاده از کد اسمبلی RDTSC که با استفاده از این دستور و محاسبه تاخیر اجرای آن پی به اجرای بد افزار در محیط شبیه ساز مجازی می برد (اجرای این دستور اگر در محیط شبیه ساز مجازی باشد، زمان اجرای آن بالاتر از معمول خواهد بود)

• در صورتیکه این بدافزار از حضور Virtual Machine آگاهی یابد، علاوه براینکه از آلوده‌کردن درایو قابل حمل امتناع می نماید، روند اجرای خود را به صورتی تغییر می دهد که کار اصلی مخرب کرم انجام نشود. در نهایت روال خود را به صورت زیر تغییر خواهد داد:

• به سایت http://suck****.in متصل می شود تا بتواند فایل Thumbs.db جدید را دانلودکند.

• روی پورت ۱۶۴۱۵ برای دانلود فایل یا گرفتن دستور منتظر می ماند.

• مشخصات سیستم میزبان را گرفته و پس از کدکردن، آنرا به سایت های زیر ارسال می کند.

http://bdcr****.nl/in.php
http://xdqz****.ru/in.php
http://orzdw****.in/in.php
http://ana****.su/in.php
http://somi****.ru/in.php
http://ygiud****.in/in.php

گفتنی است که تحلیل گامارو توسط تیم تحلیل بدافزار شرکت نرم افزاری امن پرداز و در آزمایشگاه بدافزار پادویش انجام گردیده است.
شما نیز برای دیدن تحلیل های بیشتر ثبت شده توسط گروه تحلیل امن پرداز می توانید به سایت پادویش مراجعه نمایید.

http://www.padvish-antivirus.com

آیا "Viber" هک شد ؟!

یکی از زیردامنه های معروفترین برنامه رایگان گفت وگوی گوشی های هوشمند یعنی "وایبر :Viber" توسط ارتش الکترونیکی سوریه -SEA- هک شد. به گفته ی این گروه، تنها بخشی از پایگاه داده وب سایت این برنامه هک شده است.

این گروه به کاربران این برنامه پیشنهاد نموده است که برنامه را در گوشی های خود غیرفعال نمایند، زیرا شرکت "Viber" تمامی کاربران خود را استراق سمع می نماید و همچنین آدرس IP و شماره ی تلفن هر کاربر را داخل پایگاه داده خود ذخیره می نماید. پس از وقوع این حمله، شرکت "Viber" به تمامی کاربران خود اعلام نمود که داده های این شرکت ایمن می باشد. آنها این حمله را بدین گونه توضیح داده اند که تنها وب سایت پشتیبانی "Viber" مورد حمله قرار گرفته بود، که به دلیل حمله فیشینگی (Phishing) است که بر روی یکی از کارمندان "Viber" صورت گرفته بود. همچنین این نوع حمله، امکان دسترسی به دو سیستم را داده است:

۱-پنل پشتیبانی کاربر ۲-سیستم پشتیبانی ادمین

و اطلاعات از یکی از این دو سیستم ارسال گردیده است.

نکته مهمی که در اینجا مطرح می باشد این است، که اثبات شود هیچ داده حساسی افشاء نگردیده وپایگاه های داده "Viber" هک نشده است. به گفته این شرکت اطلاعات حساس و خصوصی کاربران در سیستمی امن نگه داری می شود، که از طریق اینگونه حملات قابل دسترسی نمی باشد. به علاوه این شرکت اعلام نمود که در حال بازنگری سیاست های خود به منظور حصول اطمینان از عدم تکرار این گونه حوادث در آینده می باشند.

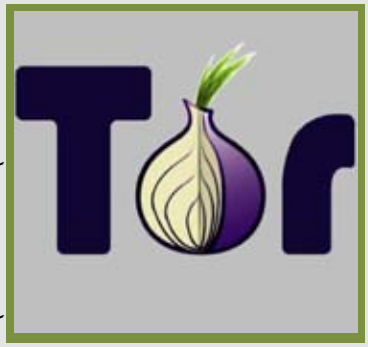
پیگیری تلفن همراه خاموش

آژانس امنیت ملی ایالات متحده ی آمریکا بیان نموده است که قادر به ردیابی تلفن همراه حتی در صورت خاموشی آن می باشد. این تکنیک که پیش تر توسط این آژانس کشف شده بود، در ۲۰ جولای ۲۰۱۳ توسط خبرگزاری ها اعلام گردید.

یکی از کارشناسان امنیت اعلام نمود که تلفن های همراه هوشمند در زمان خاموشی، به صورت ۱۰۰٪ خاموش نیستند و تنها با خارج نمودن باتری آن می توان اطمینان حاصل کرد که خاموش شده اند. همچنین بهترین راه به منظور ردیابی یک تلفن همراه خاموش، جاگذاری تراشه در داخل باتری تلفن می باشد که در صورت خاموش بودن تلفن همراه نیز این تراشه روشن بماند. البته در این حالت، تلفن همراه قابل پیگیری نیست و فقط تراشه قابل پیگیری می باشد.

اما تلفن های همراه قدیمی در صورت خاموش بودن، به صورت ۱۰۰٪ خاموش نمی شوند. به عنوان مثال زمانی که یک تلفن همراه قدیمی خاموش می شود، به دلیل وجود یک پردازنده که هر ۱۰ دقیقه بالا می آید امکان دریافت پیام کوتاه وجود دارد اما امکان دریافت تماس تلفنی ندارد.

بدین ترتیب این فرضیه که تلفن های همراه خاموش قابل پیگیری هستند با توجه به نوع تلفن همراه متفاوت می باشد.



خطر در کمین کاربران برنامه TOR

شرکت Freedomweb که خدمات میزبانی وب را برای سرویس های Tor فراهم می نمود، متوقف گردید. دلیل توقف شبکه ی این شرکت به دلیل اتهاماتی است که به مالک این شرکت –اریک مارکس– وارد شده است.

کاربران این سرویس ها اعلام نموده اند که کپی های موجود مرورگر Tor که اکثر افراد از آنها استفاده می نمایند، آلوده به کدهای مخرب جاوا اسکریپت می باشد. لازم به ذکر است که در نسخه های قدیمی مرورگر Tor، جاوا اسکریپت غیرفعال بوده، اما این ویژگی به دلیل استفاده ی زیاد در مرورگر فعال شده است. این آسیب پذیری، برای مرورگر فایرفاکس در سیستم عامل ویندوز و جهت به خطرانداختن هویت کاربران صورت گرفته است.

لازم به ذکر است که این آسیب پذیری برای شناسایی افراد متخلف توسط پلیس فدرال به کار می رود.

Plugx و تحلیل آن در آزمایشگاه بدافزار پادویش

Plugx ابزاری برای دسترسی از راه دور به سیستم آلوده یا همان RAT است که نویسندگان بدافزار با استفاده از آن به دزدی اطلاعات حساس کاربران پرداخته و سیستم را تحت کنترل خود درمی‌آورند. این بدافزار از طریق ایمیل منتشر می‌شود و برای نصب شدن در سیستم، از شکاف های امنیتی برروی نرم افزارهایی چون pdf و office و در نمونه های جدیدتر از خود IExplorer استفاده می نماید.
به گفته ی آزمایشگاه بدافزار پادویش، این بدافزار با اجراکردن و استفاده از فایل امضا شده توسط شرکت های شناخته شده، به بارگذاری کدهای مخرب خود می پردازد. Plugx در پردازه های قانونی تزریق انجام داده تا به صورت پنهانی به اجرای کدهای مخرب خود بپردازد. این بدافزار با اتصال به سرور، دستوراتی را دریافت کرده و با استفاده از ماژول های خود، به اجرای این دستورات می پردازد.
علی رقم تمام این هوشمندی ها، این بدافزار تا کنون در نسخه ی آزمایشی می باشد، پس آمادگی دریافت نسخه ی تکمیل شده ی آن را داشته باشید!

بدافزارها در سیستم کنترل پاسپورت استانبول

سیستم کنترل پاسپورت فرودگاه بین المللی آتاتورک استانبول، چندی پیش مورد حمله سایبری قرار گرفته بود. این در حالیست که این حمله بر روی فرودگاه های دیگر ترکیه نیز تاثیر گذاشته است.
خبرگزاری های محلی اعلام نموده اند که سیستم کنترل پاسپورت فرودگاه سبیها-"Sabiha"- دراستانبول از کار افتاده، که علت آن بد عمل نمودن یکی از سیستم ها گزارش شده است .
مسئولان امنیت شبکه های کامپیوتری فرودگاه معتقدند که سیستم ها توسط بدافزارها آلوده گشته اند. البته تاکنون هیچ گروهی و یا شخصی به عنوان مسئول این اتفاقات معرفی نگردیده، هرچند اخیرا گزارش های دیگری نیز مبنی بر این نوع حملات منتشر گردیده است.

پایان "XP" پس از ۱۳ سال ...

چندی پیش، مایکروسافت به کاربران ویندوز XP هشدار داد درصورتی‌که پیش از آوریل ۲۰۱۴ به استفاده از این سیستم عامل پایان ندهند، با آسیب پذیری هایی روبرو خواهند شد که هرگز ترمیم نمی شود. این هشدار که آخرین هشدار در کمپین دوساله متقاعد کردن کاربران برای کنار گذاشتن ویندوز XP است، مشابه هشداری است که SANS مبنی بر این پیش‌بینی منتشر نمود، که هکرها آسیب پذیری های شناسایی شده ویندوز XP را تا زمانی که مایکروسافت پشتیبانی این سیستم عامل را قطع کند، نگاه خواهند داشت و پس از آن اقدام به سوء استفاده از این آسیب پذیری ها بر روی سیستم های محافظت نشده خواهند کرد.
انتظار می رود در اولین ماه‌ها پس از آوریل ۲۰۱۴ با عرضه به‌روز رسانی های امنیتی مایکروسافت، مهاجمان این به‌روز رسانی ها را مهندسی معکوس کرده و آسیب‌پذیری‌ها را کشف نموده و بر روی ویندوز XP تست کنند. درصورتی‌که ویندوز XP نیز این آسیب‌پذیری ها را داشته باشد، مهاجمان تلاش خواهند کرد کد سوء استفاده کننده از این آسیب‌پذیری ها را در ویندوز XP تولید کنند. از آنجایی‌که از آن پس هیچ به‌روزرسانی امنیتی برای ویندوز XP عرضه نخواهد شد، این آسیب‌پذیری ها همواره اصلاح نشده باقی خواهند ماند.
مهندسی معکوس اصلاحیه‌ها یک روش معمول مورد استفاده محققان امنیتی و مجرمان سایبری است. زمانی که اصلاحیه‌ای عرضه می‌شود، هکرها می‌توانند با مقایسه ی کد نسخه‌های به‌روز رسانی شده و به‌روز نشده، تغییرات را شناسایی کنند. به این ترتیب محل وقوع آسیب‌پذیری ها مشخص می‌شود. در نهایت آنها می‌توانند از این اطلاعات برای بررسی وجود این آسیب‌پذیری ها در ویندوز XP استفاده کنند.

مدیریت امنیت اطلاعات

بخش سوم

در شماره‌های پیشین به تعریف مفهومی کلی از سیستم مدیریت امنیت اطلاعات، بیان مراحل آن و سپس تفضیل مرحله‌ی اول سیستم مدیریت امنیت اطلاعات پرداخته شده است.
در این شماره به مرحله‌ی دوم سیستم مدیریت امنیت اطلاعات پرداخته می‌شود.

فاز اجرا:
در فاز طرح، راهنمایی‌هایی در جهت پیاده سازی ISMS، با توجه به اقدامات پیاده‌سازی در فاز اجرا، تولید می‌گردد. هسته‌ی اصلی فاز اجرا، پیاده‌سازی نتیجه‌ی طرح مقابله با خطر و از فرآیندهای مدیریت ریسک می‌باشد. استانداردهای ISO 27002 و ISO 27001، راهنمایی در جهت پیاده‌سازی کنترل‌های امنیتی ندارد. اما استاندارد ISO 2700 مورد استفاده و اجرای مدل PDCA به منظور ایجاد، طرح‌ریزی، پیاده سازی و اجرای ISMS، راهنمایی‌هایی را به همراه جزییات بیان نموده است.
پیاده‌سازی طرح مقابله با خطر با تعیین سیاست‌هایی آغاز می‌گردد. مواردی همچون چگونگی پیاده سازی سیاست‌ها و اینکه چه مواردی در پیاده‌سازی آنها به کار برود، در استاندارد بیان گشته است.

۱. طرح مقابله با خطر
طرح مقابله با خطر در ابتدا خطرات موجود در سازمان را مشخص نموده و سپس مسئولیت‌های سازمانی به منظور مقابله با آنها را بیان می‌نماید. همچنین این طرح نقش‌ها و مسئولیت‌ها را در ایجاد استراتژی مدیریت خطر، اقدامات مدیریتی در تبدیل استراتژی‌ها به تاکتیک‌ها، نظارت، کنترل و گزارش فعالیت‌های مدیریتی شرح می‌دهد.

-نوشتن سیاست‌ها
سیاست ISMS و سیاست‌های سازمانی به اهمیت امنیت در سازمان اشاره می‌نماید. اولین قدم در فاز اجرا توسعه و ایجاد سیاست‌هایی برای کنترل امنیتی می‌باشد. لازم به ذکر است که این سیاست‌ها هیچ کنترل امنیتی خاصی را شناسایی نمی‌نماید. اما سیاست‌های ایجاد شده باید به گونه‌ای باشد که تمامی کنترل‌های ISO را تحت پوشش قرار می‌دهد.
لازم به یادآوری می‌باشد که سیاست‌های مقررشده باید واضح، کوتاه و قابل پیاده‌سازی بوده و همچنین تمامی کنترل‌های ISO در آن قابل مشاهده باشد.

۲. انتخاب و پیاده‌سازی کنترل‌ها
به منظور انتخاب و پیاده‌سازی کنترل‌های مناسب، از استاندارد ISO 27002 به عنوان قالب و راهنما استفاده می‌شود. در این مرحله دلایل انتخاب و عدم انتخاب کنترل‌ها به تفکیک ذکر می‌گردد و نتیجه‌ی این اقدام سند SOA است. در انتخاب کنترل‌ها توجه به این نکته که "چه ویژگی خاصی از این کنترل را سازمان نیاز دارد؟" ضروری است.

۳. آگاهی و آموزش
به طور کلی فرآیند آموزش شامل آگاهی، ادراک و استفاده می‌باشد. همچنین انسان‌ها آغاز به دانستن چیزی نمی‌کنند که از آن آگاهی ندارند. اما آگاهی این کمبود را از بین می‌برد.
آگاهی امنیت دانشی در مورد امنیت فراهم می‌نماید. زمانی که افراد یک سازمان این موضوع را به درستی درک کنند، بیشتر به امنیت و نقش خود در این موضوع توجه می‌نمایند. با استفاده از این مهارت‌ها، افراد در اقدامات و فعالیت‌های خود به امنیت اهمیت داده و آن را پیاده‌سازی می‌نمایند.

جمع آوری اطلاعات در
آزمون نفوذپذیری
بخش سوم

در آزمون نفوذپذیری اولین گام پس از برنامه ریزی ، جمع‌آوری اطلاعات می باشد که از اهمیت ویژه‌ای برخوردار است. در پایان این فاز، نقشه‌ای کامل از شبکه‌ی هدف بدست می‌آید. همچنین آزمون کننده قادر به شناسایی سیستم های موجود در شبکه می باشد.
جمع آوری اطلاعات به دو صورت انجام می پذیرد: غیرفعال و فعال.
در جمع‌آوری اطلاعات به صورت غیرفعال، آزمون کننده سعی در جمع آوری اطلاعاتی درباره هدف بدون ارتباط مستقیم با آن را دارد. همچنین با توجه به هدف از آزمون نفوذ ، آزمون کننده سعی در جمع‌آوری اطلاعاتی مانند مالکیت سازمان هدف ، مکان و محل آن، مکان شبکه و سیستم های آن را دارد.
در جمع آوری اطلاعات به صورت فعال، آزمون‌کننده به هدف متصل می‌گردد. هدف از جمع آوری اطلاعات بدین طریق به این دلیل می باشد که درک بهتری از هدف به دست می‌آید . به عنوان مثال می‌توان به مشخص شدن نوع و تعداد سیستم های موجود در سازمان هدف اشاره کرد.
در ادامه هر یک از این روش ها به تفصیل توضیح داده شده‌اند:

• جمع آوری اطلاعات به صورت غیرفعال

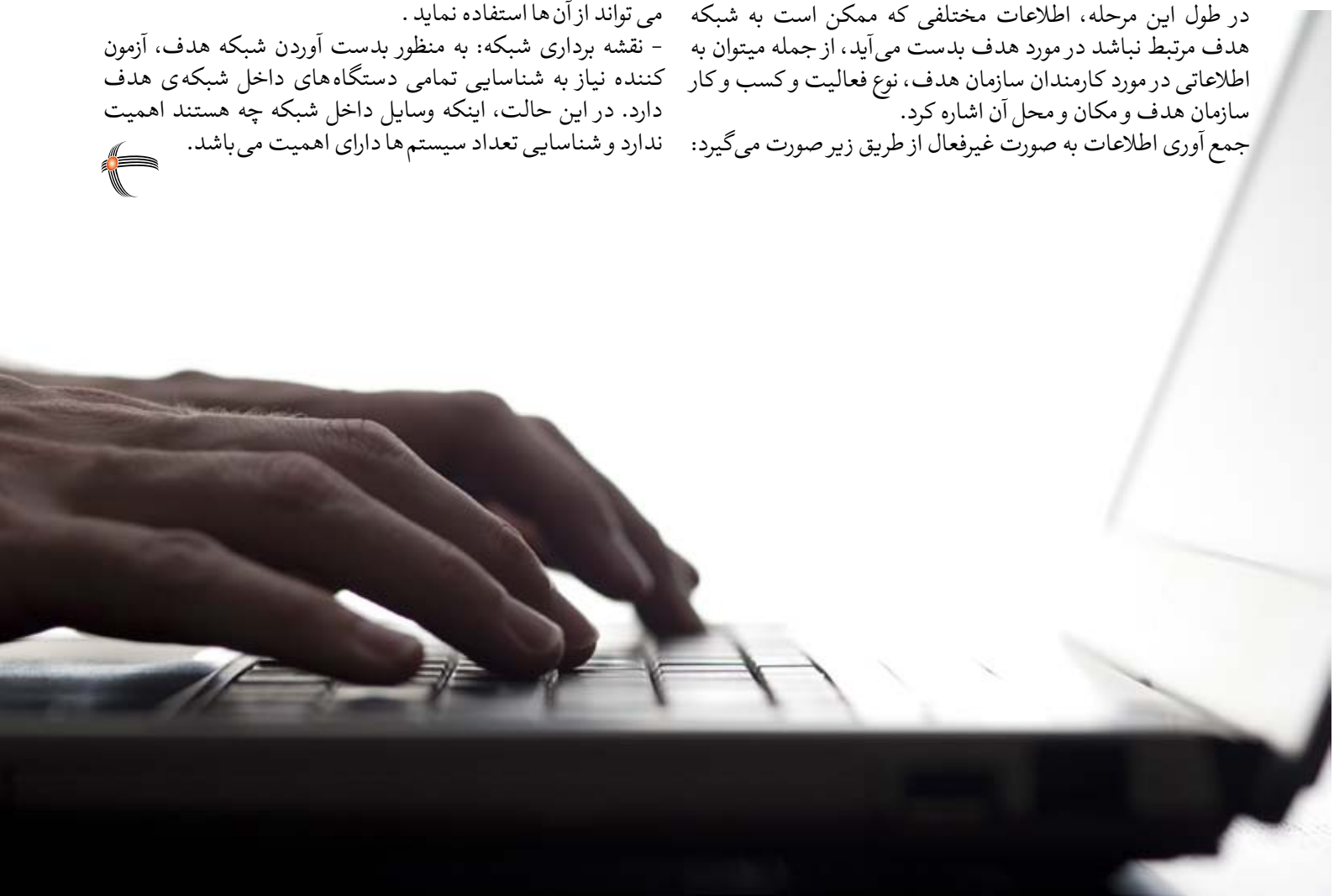
در طول این مرحله، اطلاعات مختلفی که ممکن است به شبکه هدف مرتبط نباشد در مورد هدف بدست می‌آید، از جمله میتوان به اطلاعاتی در مورد کارمندان سازمان هدف، نوع فعالیت و کسب و کار سازمان هدف و مکان و محل آن اشاره کرد.
جمع آوری اطلاعات به صورت غیرفعال از طریق زیر صورت می‌گیرد:

- جمع آوری اطلاعات در مورد هدف، توسط موتورهای جستجو
- جستجو در گروههایی که شامل کارمندان سازمان هدف می باشد
- جستجو در وب سایت های شخصی کارمندان سازمان هدف
- جستجو در آرشیو سایت سازمان هدف به منظور جمع آوری اطلاعات
- جستجو در گروه های خبری

در پایان این مرحله ، آزمون‌کننده اطلاعات با ارزشی در مورد شبکه‌ی هدف و بدون داشتن اطلاعاتی در مورد آن به دست می‌آورد .

• جمع آوری اطلاعات به صورت فعال

در این مرحله آزمون کننده اطلاعاتی در مورد شبکه هدف به‌دست می‌آورد. مواردی که از این طریق بدست می‌آیند به شرح زیر است:
- اطلاعات در مورد DNS : این اطلاعات کمک به شناسایی نسخه سرور BIND هدف می‌کند. همچنین آزمون‌کننده با برقراری ارتباط با سرور DNS هدف، می تواند اطلاعات بسیاری را جمع‌آوری نماید.
- حساب های پست الکترونیکی: در صورت وجود سرور پست الکترونیکی بر روی هدف، آزمون کننده قادر به تهیه لیستی از کاربران آن بوده و در حملات همچون حمله brute force و مهندسی اجتماعی می تواند از آن ها استفاده نماید .
- نقشه برداری شبکه: به منظور بدست آوردن شبکه هدف، آزمون کننده نیاز به شناسایی تمامی دستگاه‌های داخل شبکه‌ی هدف دارد. در این حالت، اینکه وسایل داخل شبکه چه هستند اهمیت ندارد و شناسایی تعداد سیستم ها دارای اهمیت می باشد.



شرکت نرم افزاری

امن پرداز

آدرس: تهران، خیابان ملاصدرا، خیابان شیخ بهایی جنوبی، گرمسار غربی، پلاک ۷۶
تلفن: ۷-۸۸۰۶۹۶۴۵-۰۲۱-۸۸۰۳۵۵۸۱ فکس: ۰۲۱-۸۸۶۰۵۰۴۶
www.amnpardaz.com
info@amnpardaz.com